

1 Claims 1-3, 5, 14-17, 22 and 28-32 are amended.

2 Claims 6-7 and 18 are cancelled.

3 Claims 1-5, 8-17 and 19-32 remain in the Application as follows:

4
5 **1. (Currently Amended)** A method comprising:

6 receiving an event from a first security engine;

7 identifying a second security engine configured to utilize information
8 contained in the event; and

9 communicating the information contained in the event to the second
10 security engine, wherein the event corresponds to identifying a password that does
11 not comply with predetermined criteria.

12
13 **2. (Currently Amended)** A method as recited in claim 1 wherein the
14 event identifies a ~~type of security attack~~ a password that does not comply with a
15 length criteria.

16
17 **3. (Currently Amended)** A method as recited in claim 1 wherein the
18 event identifies an action performed by the first security engine in response to a
19 security attack detected vulnerability.

20
21 **4. (Original)** A method as recited in claim 1 wherein the first security
22 engine and the second security engine are application programs.

1 **5. (Currently Amended)** A method as recited in claim 1 wherein the
2 ~~first security engine is an antivirus application program~~ event identifies a
3 password that does not include one or more required characters.
4

5 **6-7. (Cancelled).**
6

7 **8. (Original)** A method as recited in claim 1 wherein the first security
8 engine is a vulnerability analysis application program.
9

10 **9. (Original)** A method as recited in claim 1 further comprising:
11 identifying a third security engine configured to utilize information
12 contained in the event; and
13 communicating the information contained in the event to the third security
14 engine.
15

16 **10. (Original)** A method as recited in claim 1 further comprising:
17 receiving an updated security policy;
18 identifying at least one security engine associated with the updated security
19 policy; and
20 providing the updated security policy to the identified security engine.
21

22 **11. (Original)** A method as recited in claim 1 further comprising:
23 receiving a request for data from the first security engine; and
24 communicating the requested data to the first security engine.
25

12. (Original) A method as recited in claim 1 further comprising
storing information contained in the event in a central location accessible to a
plurality of security engines.

13. (Original) One or more computer-readable memories containing a
computer program that is executable by a processor to perform the method recited
in claim 1.

14. (Currently Amended) A method comprising:
receiving a security-related event from a first security-related application
program, the security-related event being associated with a system state;
identifying information contained in the security-related event;
identifying a second security-related application program associated with
the information contained in the security-related event; and
communicating the information contained in the security-related event to
the second security-related application program.

15. (Currently Amended) A method as recited in claim 14 wherein the
~~first security-related application program is an antivirus application program~~
information includes whether a network connection is wired or wireless.

16. (Currently Amended) A method as recited in claim 14 wherein the
~~security-related event is associated with system-state information~~ information
includes whether a host computer is accessing a corporate network.

1 **17. (Currently Amended)** A method as recited in claim 14 wherein the
2 information contained in the security-related event includes data identifying a type
3 of security attack includes whether a host computer is accessing an unknown
4 network.

5
6 **18. (Cancelled).**

7
8 **19. (Original)** A method as recited in claim 14 further comprising:
9 receiving system state information from a third security-related application
10 program; and
11 storing the system state information such that the system state information
12 is accessible to the first security-related application program and the second
13 security-related application program.

14
15 **20. (Original)** A method as recited in claim 14 further comprising:
16 identifying a third security-related application program associated with the
17 information contained in the security-related event; and
18 communicating the information contained in the security-related event to
19 the third security-related application program.

20
21 **21. (Original)** One or more computer-readable memories containing a
22 computer program that is executable by a processor to perform the method recited
23 in claim 14.
24
25

1 **22. (Currently Amended)** A system implemented at least in part by a
2 computing device, comprising:

3 a first security engine associated with a first type of security attack, the first
4 security engine including configuration to detect a password that does not comply
5 with predetermined criteria;

6 a second security engine associated with a second type of security attack;
7 and

8 an event manager coupled to receive events from the first security engine
9 and the second security engine, the event manager further to identify information
10 contained in the events and to identify at least one security engine associated with
11 information contained in a particular event, and further to communicate the
12 information contained in the particular event to the at least one security engine.

13
14 **23. (Original)** A system as recited in claim 22 wherein the information
15 contained in the events identifies a type of security attack.

16
17 **24. (Original)** A system as recited in claim 22 wherein the information
18 contained in each event identifies an action taken in response to a security attack.

19
20 **25. (Original)** A system as recited in claim 22 wherein the information
21 contained in the events includes system state information.

22
23 **26. (Original)** A system as recited in claim 22 further comprising a
24 third security engine coupled to the event manager and associated with a third type
25 of security attack.

1 **27. (Original)** A system as recited in claim 22 further comprising a
2 storage device coupled to the event manager, the first security engine and the
3 second security engine, the storage device to store event information.

4
5 **28. (Currently Amended)** One or more tangible computer-readable
6 media having stored thereon a computer program that, when executed by one or
7 more processors, causes the one or more processors to:

8 receive a first security-related event from a first service, the first security-
9 related event corresponding to a network-related aspect of a system state;

10 identify information contained in the first security-related event;

11 receive a second security-related event from a second service;

12 identify information contained in the second security-related event;

13 communicate information contained in the first security-related event to the
14 second service; and

15 communicate information contained in the second security-related event to
16 the first service.

17
18 **29. (Currently Amended)** One or more tangible computer-readable
19 media as recited in claim 28 wherein the first security-related event identifies a
20 particular type of security attack.

21
22 **30. (Currently Amended)** One or more tangible computer-readable
23 media as recited in claim 28 wherein the one or more processors further store the
24 information contained in the first security-related event and the information
25 contained in the second security-related event for access by other services.

1 **31. (Currently Amended)** One or more tangible computer-readable
2 media as recited in claim 28 wherein the one or more processors further
3 communicate information contained in the first security-related event to a third
4 service.

5
6 **32. (Currently Amended)** One or more tangible computer-readable
7 media as recited in claim 28 wherein the first service is associated with a first type
8 of security attack and the second service is associated with a second type of
9 security attack.